Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L24	(rule$1 or condition?) same (co-brows$ or (colaborat$ adj2 brows$))	0	L24
L23	(rule$1 or condition?) with (co-brows$ or (colaborat$ adj2 brows$))	0	L23
DB=USPT; PLUR=YES; OP=OR			
L22	(rule$1 or condition?) same (co-brows$ or (colaborat$ adj2 brows$))	0	L22
L21	(rule$1 or condition?) with (co-brows$ or (colaborat$ adj2 brows$))	0	L21
L20	L19 (notif$ with user$1 with characteristic$ with (share$ or common)).clm.	9	L20
L19	L18 and @ad<=19990601	9	L19
L18	(notif$ with user$1 with characteristic$).clm.	9	L18
L17	(determin$ or identif$ or select$) and (brows$ with patern$ with user$)	0	L17
L16	(determin$ or identif$ or select$) same (brows$ with patern$ with user$)	0	L16
L15	L13 and (first adj user) and (second adj user)	11	L15
L14	L12 @ad<=19990601	2804852	L14
L13	L12 and @ad<=19990601	213	L13
L12	(monitor$ with brows$ with user$)same user$	243	L12
L11	(monitor$ with brows$ with patern$) and user$	0	L11
L10	(monitor$ with brows$ with patern$)	0	L10
L9	(monitor$ with brows$ with patern$ with user$)	0	L9
L8	(monitor? with brows$ with patern$ with user$)	0	L8
L7	(monitor? with brows$ with patern$ with user$).clm.	0	L7
L6	L5 and l1	6	L6
L5	6081900.pn. or 6029195.pn. or 5931912.pn. or 5835087.pn. or 5754939.pn. or 5754938.pn.	6	L5
L4	L3 and (internet or www or web)	6	L4
L3	L2 and l1	6	L3
L2	L1 @ad<=19990601	2804822	L2
L1	(proxy near2 server$1) same (protect$ with identi$)	6	L1

cl. 13

END OF SEARCH HISTORY

Generate Collection | Print

L6: Entry 1 of 6 | File: USPT | Jun 27, 2000

US-PAT-NO: 6081900
DOCUMENT-IDENTIFIER: US 6081900 A

TITLE: Secure intranet access

DATE-ISSUED: June 27, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Subramaniam; Anand	San Jose	CA		
Ebrahimi; Hashem M.	Salt Lake City	UT		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Novell, Inc.	Provo	UT			02

APPL-NO: 9/ 268795 [PALM]
DATE FILED: March 16, 1999

INT-CL: [7] H04 L 9/32, G06 F 13/38

US-CL-ISSUED: 713/201; 713/153, 707/10, 707/513, 709/230, 709/245
US-CL-CURRENT: 713/201; 707/10, 707/513, 709/230, 709/245, 713/153

FIELD-OF-SEARCH: 713/151, 713/153, 713/155, 713/160, 713/162, 713/201, 709/217, 709/218, 709/214, 709/230, 709/238, 709/245, 707/10, 707/501, 707/513

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

L6: Entry 1 of 6 File: USPT Jun 27, 2000

DOCUMENT-IDENTIFIER: US 6081900 A
TITLE: Secure intranet access

Brief Summary Paragraph Right (3):
With the growth of such secure networks and their information content, there is an urgent need to support secure access by authorized users even when those users log in from a client machine outside the network security perimeter. A wide variety of tools and techniques relating to networks and/or security are known, at least individually and to at least some extent, including: computer network architectures including at least transport and session layers, sockets, clients, and servers; hyperlinks and uniform/universal resource locators (URLs); communications links such as Internet connections and LAN connections; proxy servers for HTTP and some other protocols; internetworking; Kerberos authentication; authentication through certificates exchanged during an SSL handshake; tying certificates to access control lists so that users are identified in certificates presented during the SSL handshake instead of being identified by an IP address, DNS name, or username and password; multiple instances of a server on the same machine in order to serve both insecure and secure documents; using a single password to log into an entire network rather than logging into individual servers; proxy servers as an example of servers which require user authentication; a secure sockets layer protocol manifestation in URLs, including protocol identifiers "http://" and "https://"; the use of a specific server port for network communication; various definitions of VPNs (virtual private networks); "route filtering" which controls route propagation; Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP); use of encryption technologies to provide the segmentation and virtualization required for VPN connectivity deployed in almost any layer of the protocol stack; transport or application layer VPNs; basic VPN requirements such as user authentication, address management, data encryption, key management, and multiprotocol support; tunneling by packet encapsulation, packet transmission, and packet unencapsulation; Lightweight Directory Access Protocol; a split proxy system for a protected computer network; translation between transport layer protocols; translation between IP and non-IP protocols; a proxy server within a network which receives a request for a protected Web resource from a browser outside the network and requires authentication of the browser to the proxy using some combination of a user ID and/or password; Novell/NetWare Directory Service (NDS) and user access controls; Windows NT Domain directory; Reverse Proxy/Virtual Hosting; a proxy server with HTTP caching; use of a proxy server by configuring client software to connect through the proxy server to prevent the client from being connected directly to the Internet; SSL encryption; an entry manager which serves as a single point of network entry for all users; a Trusted Sendmail Proxy, in the context of sensitivity labels and privileges, including a small, trusted program which acts as a communication path between an inside compartment that performs privileged internal operations and delivers local messages and an outside compartment that collects and send messages without privilege; a secured https proxy which apparently does SSL tunneling, logging, and reacting to events; software which apparently allows use of https URLs by way of an SSL connection with a program that wraps https calls to http; a protocol stream or content processor which knows how to convert something involving an URL into a proprietary content container which knows its content and that content's type, for HTTP, HTTPS, FTP, gopher, and other protocols; redirection of HTTP requests in connection with an HTTP proxy; superuser privileges; and object rights and property rights which apply to properties of an NDS object, as well as distribution of directory information across the network through replication.

Generate Collection | Print

L6: Entry 2 of 6 File: USPT Feb 22, 2000

US-PAT-NO: 6029195
DOCUMENT-IDENTIFIER: US 6029195 A

TITLE: System for customized electronic identification of desirable objects

DATE-ISSUED: February 22, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herz; Frederick S. M.	Davis	WV	26260	

APPL-NO: 8/ 985731 [PALM]
DATE FILED: December 5, 1997

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This patent application was originally filed as Provisional Patent Application Ser. No. 60/032,461 on Dec. 9, 1996 and is a continuation-in-part of U.S. patent application Ser. No. 08/346,425, filed Nov. 29, 1994, now U.S. Pat. No. 5,758,257 and titled "SYSTEM AND METHOD FOR SCHEDULING BROADCAST OF AND ACCESS TO VIDEO PROGRAMS AND OTHER DATA USING CUSTOMER PROFILES", which application is assigned to the same assignee as the present application.

INT-CL: [7] G06 F 15/16, H04 H 1/02, H04 N 7/14

US-CL-ISSUED: 709/219; 348/1, 455/2, 707/10
US-CL-CURRENT: 725/116; 707/10, 725/93

FIELD-OF-SEARCH: 395/200.47-200.49, 348/1, 348/2, 348/6, 348/7, 348/8, 348/10, 455/3.1, 455/4.1, 455/4.2, 455/5.1, 455/6.1, 455/6.2

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

L6: Entry 2 of 6 File: USPT Feb 22, 2000

DOCUMENT-IDENTIFIER: US 6029195 A
TITLE: System for customized electronic identification of desirable objects

Detailed Description Paragraph Right (61):
The service provider must have a means of protection from users who violate previously agreed upon terms of service. For example, if a user that uses a given pseudonym engages in activities that violate the terms of service, then the service provider should be able to take action against the user, such as denying the user service and blacklisting the user from transactions with other parties that the user might be tempted to defraud. This type of situation might occur when a user employs a service provider for illegal activities or defaults in payments to the service provider. The method of the paper titled "Security without identification: Transaction systems to make Big-Brother obsolete", published in the Communications of the ACM, 28(10), October 1985; pp.1030-1044, incorporated herein, provides for a mechanism to enforce protection against this type of behavior through the use of resolution credentials, which are credentials that are periodically provided to individuals contingent upon their behaving consistent with the agreed upon terms of service between the user and information provider and network vendor entities (such as regular payment for services rendered, civil conduct, etc.). For the user's safety, if the issuer of a resolution credential refuses to grant this resolution credential to the user, then the refusal may be appealed to an adjudicating third party. The integrity of the user profiles and target profile interest summaries stored on proxy servers is important: if a seller relies on such user-specific information to deliver promotional offers or other material to a particular class of users, but not to other users, then the user-specific information must be accurate and untampered with in any way. The user may likewise wish to ensure that other parties not tamper with the user's user profile and target profile interest summary, since such modification could degrade the system's ability to match the user with the most appropriate target objects. This is done by providing for the user to apply digital signatures to the control messages sent by the user to the proxy server. Each pseudonym is paired with a public cryptographic key and a private cryptographic key, where the private key is known only to the user who holds that pseudonym; when the user sends a control message to a proxy server under a given pseudonym, the proxy server uses the pseudonym's public key to verify that the message has been digitally signed by someone who knows the pseudonym's private key. This prevents other parties from masquerading as the user.

Detailed Description Paragraph Right (86):
Although users' true identities are protected by the use of secure mix paths, pseudonymity does not guarantee complete privacy. In particular, advertisers can in principle employ user-specific data to barrage users with unwanted solicitations. The general solution to this problem is for proxy server S2 to act as a representative on behalf of each user in its user base, permitting access to the user and the user's private data only in accordance with criteria that have been set by the user. Proxy server S2 can restrict access in two ways:

Generate Collection | Print

L6: Entry 3 of 6 | File: USPT | Aug 3, 1999

US-PAT-NO: 5931912
DOCUMENT-IDENTIFIER: US 5931912 A

TITLE: Traversal path-based approach to understanding user-oriented hypertext object usage

DATE-ISSUED: August 3, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Wu; Kun-Lung	Yorktown Heights	NY		
Yu; Philip Shi-Lung	Chappaqua	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 8/ 708004 [PALM]
DATE FILED: August 9, 1996

PARENT-CASE:
RELATED APPLICATIONS The present invention is related to co-pending U.S. patent application Ser. No. 08/525,891, entitled "A Fast Method for Mining Path Traversal Patterns", by Ming-Scan Chen and Philip S. Yu, filed Sep. 8, 1995, IBM Docket No. YO995-119, which is commonly assigned to the assignee of the present invention, and is hereby incorporated by reference in its entirety .

INT-CL: [6] G06 F 17/00

US-CL-ISSUED: 709/224
US-CL-CURRENT: 709/224

FIELD-OF-SEARCH: 395/200.54, 395/200.33, 395/200.59, 395/187.01, 395/200.48, 364/284.4, 364/200.57, 364/242.94, 364/280, 709/224

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5355487	October 1994	Keller et al.	395/650

OTHER PUBLICATIONS

Computer Networks, Tanenbaum, Prentice-Hall, 1981, p. xiv, 36 and 86, 1981.
Dictiornary of Computing, Oxford University Press, 1996.

DOCUMENT-IDENTIFIER: US 5931912 A
TITLE: Traversal path-based approach to understanding user-oriented hypertext object usage

Detailed Description Paragraph Right (1):
FIG. 1 is a block diagram of a stateliness hypertext server system 5 that provides services to a plurality of clients 3 through a data communication network 4. An example of such a system is a World Wide Web server using the Hypertext Transfer Protocol 11 (HTTP) to provide hypertext objects to various clients through the Internet. A client system 3 typically uses a software browser 2 to retrieve and display hypertext objects 1 through the communication network 4. Often, client systems 3 are hidden behind a proxy server 10, also called a firewall, between them and the data communication network 4. A proxy server is a firewall which can protect client identities from the network. A client can also be directly connected to the data communication network without a proxy server. In any case, the communications between the client and the server are typically stateliness, i.e., after the requested hypertext objects are sent to the client from the server, the connection is dropped. The server treats each hypertext request as a brand new request without prior context.

Generate Collection | Print

L6: Entry 4 of 6 File: USPT Nov 10, 1998

US-PAT-NO: 5835087
DOCUMENT-IDENTIFIER: US 5835087 A

TITLE: System for generation of object profiles for a system for customized electronic identification of desirable objects

DATE-ISSUED: November 10, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herz; Frederick S. M.	Davis	WV	26260	
Eisner; Jason M.	Philadelphia	PA	19107	
Ungar; Lyle H.	Philadelphia	PA	19103	

APPL-NO: 8/ 551201 [PALM]
DATE FILED: October 31, 1995

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This patent application is a continuation-in-part of U.S. patent application Ser. No. 08/346,425, filed Nov. 29, 1994 and titled "SYSTEM AND METHOD FOR SCHEDULING BROADCAST OF AND ACCESS TO VIDEO PROGRAMS AND OTHER DATA USING CUSTOMER PROFILES", now U.S. Pat. No. 5,758,257, which application is assigned to the same assignee as the present application.

INT-CL: [6] H04 N 7/14

US-CL-ISSUED: 345/327; 348/1, 348/7, 348/10, 348/12, 348/13, 455/2, 455/4.2, 455/5.1

US-CL-CURRENT: 345/810; 725/14, 725/35, 725/46

FIELD-OF-SEARCH: 348/1, 348/2, 348/6, 348/7, 348/10, 348/12, 348/13, 348/906, 455/2, 455/3.1, 455/4.1, 455/4.2, 455/5.1, 455/6.1, 455/6.2, 455/6.3

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

L6: Entry 4 of 6 File: USPT Nov 10, 1998

DOCUMENT-IDENTIFIER: US 5835087 A
TITLE: System for generation of object profiles for a system for customized electronic identification of desirable objects

Detailed Description Paragraph Right (153):
Although users' true identities are protected by the use of secure mix paths, pseudonymity does not guarantee complete privacy. In particular, advertisers can in principle employ user-specific data to barrage users with unwanted solicitations. The general solution to this problem is for proxy server S2 to act as a representative on behalf of each user in its user base, permitting access to the user and the user's private data only in accordance with criteria that have been set by the user. Proxy server S2 can restrict access in two ways:

Generate Collection | Print

L6: Entry 5 of 6 File: USPT May 19, 1998

US-PAT-NO: 5754939
DOCUMENT-IDENTIFIER: US 5754939 A

TITLE: System for generation of user profiles for a system for customized electronic identification of desirable objects

DATE-ISSUED: May 19, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herz; Frederick S. M.	Davis	WV	26260	
Eisner; Jason M.	Philadelphia	PA	19107	
Ungar; Lyle H.	Philadelphia	PA	19103	
Marcus; Mitchell P.	Philadelphia	PA	19119	

APPL-NO: 8/ 551197 [PALM]
DATE FILED: October 31, 1995

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This patent application is a continuation-in-part of U.S. patent application Ser. No. 08/346,425, filed Nov. 28, 1994 and titled "SYSTEM AND METHOD FOR SCHEDULING BROADCAST OF AND ACCESS TO VIDEO PROGRAMS AND OTHER DATA USING CUSTOMER PROFILES", which application is assigned to the same assignee as the present application.

INT-CL: [6] H04 H 1/00, H04 N 7/10, H04 N 7/14, H01 J 13/00

US-CL-ISSUED: 455/4.2; 348/2, 348/7, 348/10, 348/12, 395/200.49, 455/5.1
US-CL-CURRENT: 455/3.04; 707/501.1, 709/219, 725/34

FIELD-OF-SEARCH: 455/3.1, 455/4.1, 455/4.2, 455/5.1, 455/6.1, 455/6.2, 348/1, 348/2, 348/6, 348/7, 348/8, 348/10, 348/11, 348/12, 348/13, 395/200.47, 395/200.48, 395/200.49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

L6: Entry 5 of 6 File: USPT May 19, 1998

DOCUMENT-IDENTIFIER: US 5754939 A
TITLE: System for generation of user profiles for a system for customized electronic identification of desirable objects

Detailed Description Paragraph Right (79):
Although users' true identifies are protected by the use of secure mix paths, pseudonymity does not guarantee complete privacy. In particular, advertisers can in principle employ user-specific data to barrage users with unwanted solicitations. The general solution to this problem is for proxy server S2 to act as a representative on behalf of each user in its user base, permitting access to the user and the user's private data only in accordance with criteria that have been set by the user. Proxy server S2 can restrict access in two ways:

End of Result Set

Generate Collection | Print

L6: Entry 6 of 6 File: USPT May 19, 1998

US-PAT-NO: 5754938
DOCUMENT-IDENTIFIER: US 5754938 A

TITLE: Pseudonymous server for system for customized electronic identification of desirable objects

DATE-ISSUED: May 19, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herz; Frederick S. M.	Davis	WV	26260	
Eisner; Jason M.	Philadelphia	PA	19107	
Salganicoff; Marcos	Philadelphia	PA	19130	

APPL-NO: 8/ 550886 [PALM]
DATE FILED: October 31, 1995

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This patent application is a continuation-in-part of U.S. patent application Ser. No. 08/346,425, filed Nov. 29, 1994 and titled "SYSTEM AND METHOD FOR SCHEDULING BROADCAST OF AND ACCESS TO VIDEO PROGRAMS AND OTHER DATA USING CUSTOMER PROFILES", which application is assigned to the same assignee as the present application.

INT-CL: [6] H01 H 1/00, H04 N 7/14, H04 N 7/173, H01 J 13/00

US-CL-ISSUED: 455/4.2; 349/2, 349/5.5, 349/7, 349/12, 395/200.49, 455/5.1, 380/9
US-CL-CURRENT: 725/116; 705/74, 707/6, 707/9, 709/219, 713/155, 725/1, 725/129, 725/25

FIELD-OF-SEARCH: 455/3.1, 455/4.1, 455/4.2, 455/5.1, 455/6.1, 455/6.2, 348/1, 348/2, 348/6, 348/7, 348/8, 348/10, 348/11, 348/12, 348/13, 348/5.5, 395/200.47, 395/200.48, 395/200.49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE DATE	PATENTEE-NAME	US-CL
☐	4529870	July 1985	Chaum	235/380
☐	4706080	November 1987	Sincoskie	340/825
☐	4759063	July 1988	Chaum	380/30
☐	4914698	April 1990	Chaum	380/30
☐	4926480	May 1990	Chaum	380/23
☐	4947430	August 1990	Chaum	380/25
☐	4987593	January 1991	Chaum	380/3
☐	5131039	July 1992	Chaum	380/23
☐	5136501	August 1992	Silverman et al.	364/408
☐	5230020	July 1993	Hardy et al.	455/21
☐	5245420	September 1993	Harney et al.	455/4.2
☐	5245656	September 1993	Loeb et al.	380/23
☐	5251324	October 1993	McMullan, Jr.	455/2
☐	5276736	January 1994	Chaum	380/24
☐	5301109	April 1994	Landauer et al.	364/419
☐	5321833	June 1994	Chang et al.	395/600
☐	5331554	July 1994	Graham	364/419.07
☐	5331556	July 1994	Black, Jr.et al.	364/419.01
☐	5373558	December 1994	Chaum	380/23
☐	5410344	April 1995	Graves et al.	348/1
☐	5469206	November 1995	Strubbe et al.	348/7
☐	5483278	January 1996	Strubbe et al.	348/7
☐	5534911	July 1996	Levitan	348/1
☐	5541638	July 1996	Story	348/7
☐	5600364	February 1997	Hendricks et al.	348/1

OTHER PUBLICATIONS

Tak W. Yan & Hector Garcia-Molina, SIFT--A Tool for Wide-Area Information Dissemination, 1995 USENIX Technical Conference, New Orleans, LA., Jan. 16-20, pp. 177-186.
Masahiro Morita & Yoichi Shinoda, Information Filtering Based on User Behavior Analysis and Best Match Text Retrieval, Proceedings of the Seventeenth Annual Internatonal ACM-SIGIR Conference on Research and Development in Information Retrieval, Dublin, Jul. 3-6, 1994, Pages Title p. (272)-281.
Jim Binkley & Leslie Young, Rama: An Architecture for Internet Information Filtering, Journal of Intelligent Information Systems: Integrating Artificial and Database Technologies, vol. 5, No. 2, Sep. 1995, pp. 81-99.
Foltz, P.W., Dumais, S.T., "Personalized Information Delivery: An Analysis Of Information Filtering Methods", Communications of the ACM, Dec. 1992, vol. 35, No. 12, pp. 51-60.
Belkin, N.J., Croft, W.B., "Information Filtering And Information Retrieval: Two Sides of the Same Coin?", Communications of the ACM, Dec. 1992, vol. 35, No. 12, pp. 29-38.
Chalmers, M., Chitson, P., "Bead: Explorations In Information Visualization", 15th Ann. Int'l SIGIR "92/Denmark--Jun. 1992, pp. 330-337.
Willett, P., "Recent Trends In Hierarchic Document Clustering: A Critical Review",

End of Result Set

Generate Collection | Print

L6: Entry 6 of 6 File: USPT May 19, 1998

DOCUMENT-IDENTIFIER: US 5754938 A
TITLE: Pseudonymous server for system for customized electronic identification of desirable objects

Detailed Description Paragraph Right (81):
Although users' true identities are protected by the use of secure mix paths, pseudonymity does not guarantee complete privacy. In particular, advertisers can in principle employ user-specific data to barrage users with unwanted solicitations. The general solution to this problem is for proxy server S2 to act as a representative on behalf of each user in its user base, permitting access to the user and the user's private data only in accordance with criteria that have been set by the user. Proxy server S2 can restrict access in two ways: